TURNING DATA INTO ACTIONABLE IN-TELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANA-

CIRCL / TEAM MISP PROJECT



NSPA



Turning data into actionable intelligence

05

2022-08



NSPA

THE AIM OF THIS PRESENTATION

ဗ္ပ Turning data into actionable intelligence

L The aim of this presentation

Why is contextualisation important?
 What options do we have in MISP?
 How can we leverage this in the end?

- Why is **contextualisation** important?
- What options do we have in MISP?
- How can we **leverage** this in the end?

-08

THE GROWING NEED TO CONTEXTUALISE DATA

Contextualisation became more and more important as we as a community matured

- **Growth and diversification** of our communities
- Distinguish between information of interest and raw data
- False-positive management
- TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
- Increased data volumes leads to a need to be able to prioritise
- These help with filtering your TI based on your requirements...
- ...as highlighted by Pasquale Stirparo Your Requirements Are Not My Requirements

Turning data into actionable intelligence

└─The growing need to contextualise data

THE GROWING NEED TO CONTEXTUALISE DAT

- Contextualisation became more and more important as v as a community matured
- Growth and diversification of our communities
- Distinguish between information of interest and ra
 Ealer-meditive management
- False-positive management
 TTPs and agregate information may be prevalent co
- This and aggregate momentum may be prevalent control to raw data (risk assessment)
 Increased data volumes leads to a need to be able to
- prioritise These help with filtering your TI based on you
- These help with filtering your TI based on your requirements...
- ...as highlighted by Pasquale Stirparo Your Requirements A Not My Requirements

05

8 8 0

OBJECTIVES

Turning data into actionable intelligence

└─Objectives

05

8 8 0

2022

- Some main objectives we want to achieve when producing
- data Ensure that the information is consumable by everybody
- Ensure that the information is consumable by everybody
 That it is useful to the entire target audience
- The data is contextualised for it to be understood by everyone
- What we ideally want from our data
- We want to be able to filter data for different use-cases
 We want to be able to get as much knowledge out of the data and an analysis.
- by province
 We want to know where the data is from, how it got there why we should care

- Some main objectives we want to achieve when producing data
 - Ensure that the information is **consumable** by everybody
 - ► That it is **useful** to the entire target audience
 - The data is contextualised for it to be understood by everyone
- What we ideally want from our data
 - We want to be able to **filter** data for different use-cases
 - We want to be able to get as much knowledge out of the data as possible
 - We want to know where the data is from, how it got there, why we should care

DIFFERENT LAYERS OF CONTEXT

ဗ္မ Turning data into actionable intelligence

Different layers of context

Context added by analysts / tools
 Data that tells a story
 Encoding analyst knowledge to automatically leverage the
 above

Context added by analysts / tools

- Data that tells a story
- Encoding analyst knowledge to automatically leverage the above

80

2022-08-05 _____

Turning data into actionable intelligence —Context added by analysts / tools

CONTEXT ADDED BY ANALYSTS / TOOLS

CONTEXT ADDED BY ANALYSTS / TOOLS

EXPRESSING WHY DATA-POINTS MATTER

Turning data into actionable intelligence

08-05

2022-

Expressing why data-points matter

An IP address by itself is barely ever interesting
 We need to tell the recipient / machine why this is relevant
 All data in MISP has a bare minimum required context

- An IP address by itself is barely ever interesting
 We need to tell the recipient / machine why this is relevant
- All data in MISP has a bare minimum required context
- We differentiate between indicators and supporting data

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

• Who can receive our data? What can they do with it?

- Data accuracy, source reliability
- **Why** is this data relevant to us?
- Who do we think is behind it, what tools were used?
- What sort of motivations are we dealing with? Who are the targets?
- How can we **block/detect/remediate** the attack?
- What sort of **impact** are we dealing with?

Turning data into actionable intelligence

Broadening the scope of what sort of context we are interested in

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

Whe can receive our data? What can they do with it?
 Data scores, owner reliability
 Will be this data relevant to us?
 Who do we this its behind it, what tools were used?
 What can of metherations are we dealing with? Who are the targets?
 Encore an we block/detect/memofiate the atack?

08-05

TAGGING AND TAXONOMIES

Simple labels

- Standardising on vocabularies
- Different organisational/community cultures require different nomenclatures
- Triple tag system taxonomies
- JSON libraries that can easily be defined without our intervention

Тад	Events	Attributes	Tags
workflow:state="complete"	11	0	workflow:state="complete"
workflow:state="draft"	0	0	workflow:state="draft"
workflow:state="incomplete"	55	10	workflow:state="Incomplete"
workflow:state="ongoing"	0	0	workflow:state="ongoing"

Turning data into actionable intelligence —Context added by analysts / tools

└─Tagging and taxonomies

Simple labels Standardising on Different organis different nomene Triple tag system JSON libraries th intervention	ational/com clatures 1 - taxonomie	munity 25		
14		Exercis	ARCOURT	Teps
workfore and compared				workfore as a "compare"
workfowatate-19197				wondow ease-load"
without the transport		55	10	workfore as a subcompany.
workfowstate-'origoing'				wondow manufactored

08-05

GALAXIES

- Taxonomy tags often **non self-explanatory**
 - Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies Galaxies
 - Community driven knowledge-base libraries used as tags
 - Including descriptions, links, synonyms, meta information, etc.
 - Goal was to keep it **simple and make it reusable**
 - Internally it works the exact same way as taxonomies (stick to JSON)

B Ransor	nware galaxy	
Galaxy ID	373	
Name	Ransomware	
Namespace	misp	
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb213	41078
Description	Ransomware galaxy based on	
Version	4	
Value 🕴		Synonyms
.CryptoHasYou.		
777		Sevleg
7ev3n		7ev3n-HONE\$T

Turning data into actionable intelligence —Context added by analysts / tools

└─ Galaxies

ഹ

-80

1.13	Faxonomy tags often Example: universa For the latter, a single So we needed someti Salaxies Community driven Including descripti etc. Goal was to keep i	I understan e string wa ning new in knowledge ons, links, s t simple an	ding of tipgreen vs i s ill-suited n addition to taxon -base libraries used aynonyms, meta info d make it reusable	iomies I as tag imatio
	 Internally it works JSON) 			nies (sti
	Internally it works		ame way as taxonom meare galaxy	nies (st
	Internally it works	D Ranso	enveure galaxy	nies (st
	Internally it works	D Ranso		nies (st
	Internally it works	D Ranso	erware galaxy	nies (st
	Internally it works	D Ranso	enveure galaxy	nies (st
	Internally it works	Ranso Anno	envere galaxy	nies (st
	Internally it works	Rarato Annual Annual Annual Annual Annual Annual Annual Annual Annual	enviare galaxy ¹⁰ Marcent ¹⁰	nies (s

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

- Standardising on high-level TTPs was a solution to a long list of issues
- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our filtering and situational awareness needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
 - attck4fraud ¹ by Francesco Bigarella from ING
 - **Election guidelines**² by NIS Cooperation Group

¹https://www.misp-project.org/galaxy.html#_attck4fraud ²https:

//www.misp-project.org/galaxy.html#_election_guidelines

Turning data into actionable intelligence

└─The emergence of ATT&CK and similar galaxies THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

- Standardising on high-level TTPs was a solution to a long lis of issues
 Adoption was rapid, tools producing ATT&CK data, familiar
- A much better take on kill-chain phases in general
 Feeds into our filtering and situational awareness needs
- extremely well Gave rise to other, ATT&CK-like systems tackling other concerns
- attckufraud ¹ by Francesco Bigarella from ING
 Election guidelines ² by NIS Cooperation Group

-80

DATA THAT TELLS A STORY

Turning data into actionable intelligence

2022-

DATA THAT TELLS A STORY

More complex data-structures for a modern age

- Atomic attributes were a great starting point, but lacking in many aspects
- MISP objects³ system
 - Simple **templating** approach
 - Use templating to build more complex structures
 - Decouple it from the core, allow users to define their own structures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribute types
 - Allow relationships to be built between objects

Turning data into actionable intelligence Data that tells a story

More complex data-structures for a modern age

- Atomic attributes were a great starting point, but lacking many aspects
 MISP objects² system
- MISP objects³ system
 Simple templating approact
- Simple temptating approach
 Use templating to build more complex structure
 - Decouple it from the core, allow users to define their ow stourtures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribute types
 - Allow relationships to be built between objects

https://github.com/MISP/misp-obje

³https://github.com/MISP/misp-objects

O

08-05

SUPPORTING SPECIFIC DATAMODELS

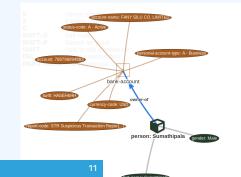
Date	Org	Category	туре		Tags	deleted attributes Galaxies	Comment	Correlate	Related Events
2018-09-28		Name: bank-accou References: 0 🖸							
2018-09-28			status-code: text	A - Active		Add			
2018-09-28			report-code: text	STR Suspicious Transaction Report		Add			
2018-09-28			personal-account-type: text	A - Business		Add			
2018-09-28			swift: bic	HASEHKHH		Add		2	3849 11320 11584
2018-09-28			account: bank-account-nr	788796894883		Add			
2018-09-28			account-name: text	FANY SILU CO. LIMITED		Add			
2018-09-28			currency-code: text	USD		Add			

2022

└─Supporting specific datamodels

PORTING SE	

Image: Constraint of the state of	 1.84		A Mark Parce Name		And and the local line	THE DESIGN
			a tata			0
		-				
-4						
			-	1	Contrast and Party	



CONTINUOUS FEEDBACK LOOP

Turning data into actionable intelligence

└─Continuous feedback loop

Data shared was frozen in time

- All we had was a creation/modification timestamp
 Improved tooling and willingness allowed us to create a
- feedback loop
- Lead to the introduction of the Sighting system
 Signal the fact of an indicator sighting...
- any action and indicator signifing...
 as well as when and where it was sighted
- Vital component for IoC lifecycle management

Data shared was frozen in time

- All we had was a creation/modification timestamp
- Improved tooling and willingness allowed us to create a feedback loop
- Lead to the introduction of the **Sighting system**
- Signal the fact of an indicator sighting...
- ...as well as when and where it was sighted
- Vital component for IoC lifecycle management

12

08-05

CONTINUOUS FEEDBACK LOOP (2)



Turning data into actionable intelligence

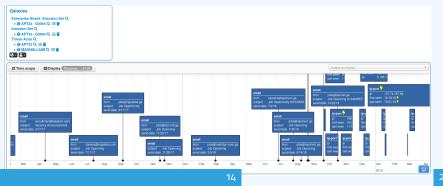
└─Continuous feedback loop (2)

Events					
•	No	GROL	2 (2017-02-19 16:17:59)		
٥	740		PN1	7	
٥	740	inted	007		
Tapa					
Owne		2015-12-34			
Thread Level		High			
Analysis		Initial			
Oatribution		Connected co	ummunideo		
Sighting Out	ah j	hered hed			
March 1		4 (k) - sobio	led to own organization only.		
CROUP		- Decesion			

08-05

A brief history of time - Adding temporality to our data

- As Andreas said no time based aspect was painful
 Recently introduced **first_seen** and **last_seen** data points
- Along with a complete integration with the **UI**
- Enables the visualisation and adjustment of indicators timeframes



Turning data into actionable intelligence \Box Data that tells a story

08-05

2022-

A brief history of time - Adding temporality to our data

A BRIEF HISTORY OF TIME - ADDING TEMPORALITY TO OUR DATA



THE VARIOUS WAYS OF ENCODING ANALYST KNOWLEDGE TO AUTOMATI-CALLY LEVERAGE OUR TI

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

2022-08-05

THE VARIOUS WAYS OF ENCODING ANALYST KNOWLEDGE TO AUTOMATI-CALLY LEVERAGE OUR TI

FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
 Lead to alert-fatigue
- Exclude organisation xy out of the community?
- FPs are often obvious can be encoded
- Warninglist system⁴ aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

ld	89	
Name	List of known IPv4 public DNS resolvers	
Description	Event contains one or more public IPv4 DNS resolvers as attribute with an IDS flag set	
Version	20181114	Warning: Potential false positives
Туре	string	······
Accepted attribute types	ip-src, ip-dst, domainjip	List of known IPv4 public DNS resolvers
Enabled	Yes (disable)	
/alues		Top 1000 website from Alexa
1.0.0.1		List of known google domains
1.1.1.1		
1.11.71.4		-

⁴https://github.com/MISP/misp-warninglists

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI — False positive handling

ഹ

-08-0

		prone information be
Lead t	o alert-fatigue	
an Annalasi	le organisation xy ou	ad the second second
E FPs an	e often obvious - can	be encoded
	nglist system ⁴ aims to	
	f well-known indicat	
	f well-known indicab positives like RFC1918	
false-p	positives like RFC1918	
false-p		
false-p	positives like RFC1918	
false-p	positives like RFC1918	
false-p	positives like RFC1918	networks,
false-p	positives like RFC1918	networks,
false-p	positives like RFC1918	networks, Warning: Potential takes
false-p	positives like RFC1918	networks, Warning: Potential takes
false-p	positives like RFC1918	Networks, Warning: Potential take p
false-p	positives like RFC1918	Networks,
false-p	positives like RFC1918	Networks, Warning: Potential take p

MAKING USE OF ALL THIS CONTEXT

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

—Making use of all this context

- Providing advanced ways of querying data
- Unified export APIs
- Incorporating all contextualisation options into API filters
 Allowing for an on-demand way of excluding potential false
- positives
 Allowing users to easily build their own export modules feed
 - lowing users to easily build their own exp eir various tools

Providing advanced ways of querying data

- Unified export APIs
- Incorporating all contextualisation options into API filters
- Allowing for an on-demand way of excluding potential false positives
- Allowing users to easily **build their own** export modules feed their various tools

-08-05

EXAMPLE QUERY

/attributes/restSearch

```
"returnFormat": "netfilter",
"enforceWarninglist": 1,
"tags": {
  "NOT":
    "tlp:white",
    "type:OSINT"
  Ι,
  "OR":
    "misp-galaxy:threat-actor=\"Sofacy\"",
    "misp-galaxy:sector=\"Chemical\""
  」,
```

Turning data into actionable intelligence The various ways of encoding analyst knowledge to automatically leverage our TI Example query

Jadoret Quisti Attributes/restSacch "restorioranis": "nesflier", "restorioranis", "topo Coll "top

EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

/events/restSearch

```
"returnFormat": "attack",
"tags": [
    "misp-galaxy:sector=\"Chemical\""
],
"timestamp": "365d"
```

Turning data into actionable intelligence

-08-05

2022

—The various ways of encoding analyst knowledge to automatically leverage our TI

Example query to generate ATT&CK heatmaps

Example query to generate ATT&CK heatmaps

/events/restSearch

"returnFormat": "attack", "tags": ["misp-galaxy:sector=\"Chemical\"], "timestamp": "t65d"

A SAMPLE RESULT FOR THE ABOVE QUERY

A SAMPLE RESULT FOR THE ABOVE QUERY

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

└─A sample result for the above query



Pre Attack - Attack Pattern	Enterprise Attack - Atta	ck Pattern Mobile Attaci	- Atlack Pattern					0		11 🛛 🖉 🕇 Show a
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Atlachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing		Password Policy Discovery	AppleScript	Data from Information Repositories	Extitution Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Extituation Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History		Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Extilitation	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestomp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obluscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modity Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software	Data from Local System		Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding

-08-05

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



Turning data into actionable intelligence

^LThe various ways of encoding analyst knowledge to automatically leverage our TI

> -Monitor trends outside of MISP (example: dashboard)



DECAYING OF INDICATORS

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making from complex filter options to complex decay models
- Decay models would take into account various available context
 - Taxonomies
 - Sightings
 - type of each indicator
 - Creation date
 - ...

Turning data into actionable intelligence 2022-08-05 -The various ways of encoding analyst knowledge to automatically leverage our TI -Decaying of indicators

We were still missing a way to use all of these systems in Move the decision making from complex filter options complex decay models

- Decay models would take into account various available

IMPLEMENTATION IN MISP: Event/view

8+ 2+												
× previous next :	• view all											
+ ≡ ≞ Date † Org	Category	le • 👕 Del Type Value	eted 🔛 Decay score 🕜 Context 🐄 Related Tags		(1) Comment Correlate	Related Feed Events hits	IDSI	Distribution	Sightings	Activity	Enter value to search Score	Q X Actions
2019-09-12	Network activity	ip-src 5.5.5.	5 🐼 + 🚨 +	🕃 + 💽 +	8		0 1	Inherit	らや♪ (000)		NIDS Simple Decaying 65.26 Model 5 79.88	••
2019-08-13	Network activity	ip-src 8.8.8.	admirally-scale-source-reliability="a" x retention:expired x	8 + 2 +	×	1222 S1:1 Show S1:2 11 more	8 1	inherit	らな♪ (5/0/0)	uul.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
2019-08-13	Network activity	ip-src 9.9.9.	9 S admirally-scale:source-reliability="c" x 9 misp:confidence-level="completely-confident" 9 tip:amber x S + +	6+ 1+ ×	×	1 3 19 S1:1 28 Show 6 more	8	inherit	合 <i>ロチ</i> (4/10)		NIDS Simple Decaying 37.43 Model 5 0	• • •

Decay score toggle button

Shows Score for each *Models* associated to the *Attribute* type

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

-08-05

2022

Implementation in MISP: Event/view

-										
				12/12			-			
			_	 12/2			*			
			-	 _			-		-	
	10000		8	 -			 27		-	
			-	_			 27	And the local division of the local division	-	
	10000	•	8	-			 27		-	
	10000	•	-	 -			 27			

Decay score toggle button
 Shows Score for each Models associated to the Attribute type

IMPLEMENTATION IN MISP: API RESULT

```
/attributes/restSearch
```

```
"Attribute": [
{
```

```
"category": "Network activity",
"type": "ip-src",
"to ids": true.
"timestamp": "1565703507",
[...]
"value": "8.8.8.8",
"decay score": [
    "score": 54.475223849544456,
    "decayed": false,
    "DecayingModel": {
      "id": "85",
      "name": "NIDS Simple Decaying Model"
```

Turning data into actionable intelligence The various ways of encoding analyst knowledge to automatically leverage our TI Implementation in MISP: API result

/attributes/restBarro *attributes/illand trypes/: "locate" "types/" injoare", "tojde": trag [...] tojde": trag [...] tojde: trag [...] tojde: tojde": trag [...] tojde: tojde": tojde: tojde: tojde": tojde: toj

TO SUM IT ALL UP...

Massive rise in user capabilities

Growing need for truly actionable threat intel

Lessons learned:

- **Context is king** Enables better decision making
- ► Intelligence and situational awareness are natural by-products of context
- Don't lock users into your workflows, build tools that enable theirs

Turning data into actionable intelligence 2022-08-05 -The various ways of encoding analyst knowledge to automatically leverage our TI

└─To sum it all up...

Massive rise in user capabilities

- Growing need for truly actionable threat in
- Lessons learned Context is king - Enables better decision making
 - Intelligence and situational awareness are natural
 - Don't lock users into your workflows, build tools that enable

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

Contact us

- https://twitter.com/mokaddem_sami
- https://twitter.com/iglocska

Contact CIRCL

- ▶ info@circl.lu
- https://twitter.com/circl_lu
- https://www.circl.lu/

Contact MISPProject

- https://github.com/MISP
- https://gitter.im/MISP/MISP
- https://twitter.com/MISPProject

Turning data into actionable intelligence —The various ways of encoding analyst knowledge to automatically leverage our TI

└─Get in touch if you have any questions

Contact us

- https://twitter.com/mokaddem_sa https://twitter.com/iglocska
- https://twitter.com/i
 Contact CIRCL
- ► info@circLlu
- https://twitter.com/circl https://www.circl.lu/
- Contact MISPProject
 https://github.com/
- https://github.com/MISP https://gitter.im/MISP/MISP

25 / 25

ഹ

2022-08-